GDPR AND FINANCIAL INSTITUTIONS: THE TOP FIVE ISSUES

Posted by Oran Gelb, Joseph Ninan on 25/05/2018

Oran Gelb
Partner, Commercial Dispute Resolution
oran.gelb@bclplaw.com

Joseph Ninan
Associate, Commercial Dispute Resolution
joseph.ninan@bclplaw.com

In this Expert Insight, Oran Gelb and Joseph Ninan comment on five aspects of the General Data Protection Regulation ((EU) 2016/679) (GDPR) that are particularly significant for financial institutions.

The General Data Protection Regulation ((EU) 679/2016/EU) (GDPR) comes into force on 25 May 2018 and represents a sea-change in the way personal data is regulated in the EU. The GDPR will have direct effect in the UK until such time as it leaves the EU, and the UK government has confirmed that it is incorporating an equivalent regime into domestic law that will continue to apply post Brexit.

Given the breadth of the personal data that they collect relating to both employees and customers, financial institutions will need to be particularly aware of their obligations under the GDPR. Those firms based outside the EU are not immune from the effects of the GDPR either. Its extra-territorial scope means that non-EU financial institutions (whether a data controller or processor), will be caught by the regime where the relevant processing activities are related to offering services to individuals within the EU.

In this article, we pick out five aspects of the GDPR that we consider are particularly significant for financial institutions.

The lawful bases for processing personal data

Under the GDPR, firms must process personal data under one of six lawful bases (Article 6(1)). There is Information Commissioner's Office (ICO) guidance that firms should consider which of the lawful bases best fits the circumstances and not simply adopt a "one-size-fits-all approach".

One of the six lawful bases is "consent". However, this is defined restrictively in Article 4(11) of the GDPR as "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies

agreement to the processing of personal data relating to him or her". Some firms that have previously relied upon consent from employees and customers on the basis of boilerplate wording in employment contracts and customer terms will likely need to find an additional base on which they can rely.

The other base most commonly relied on by firms is processing for their "legitimate interest". That base still exists under Article 6(1)(f) of the GDPR, which provides that processing will be lawful where it "is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where these interests are overridden by the interests or the fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child". Recent ICO guidance states that legitimate interests is the most flexible base for processing personal data. However, as discussed in Article, Legitimate interests under the GDPR: flexibility but at a cost reliance on this historically "business friendly" base will be subject to a greater transparency and accountability burden than previously.

Firms using the "legitimate interest" base must ensure they maintain a balance between:

→ Keeping data.

→ Erasing it.

There are many regulatory obligations that require firms to retain data, for example, provisions on record-keeping in the FCA's Senior Management Arrangements, Systems and Controls sourcebook (SYSC), obligations deriving from the senior managers and certification regime (SM&CR), and anti-money laundering (AML) requirements. A firm's compliance with such obligations will clearly fall within the scope of the legitimate interests base. However, the GDPR emphasises data minimisation. The retention of data for longer periods than is required under regulatory rules may give rise to challenges as to what constitutes legitimate interests.

Firms should reconsider blanket retention policies that allow data retention for excessive time periods. They should ensure they are able to identify all the locations in which an individual's personal data resides and are able to delete such data. Firms should also exercise particular vigilance in respect of highly sensitive personal data and ensure this type of personal data in particular is not retained for an excessive period.

Firms will now have to consider producing a documented legitimate interests assessment, explain what the legitimate interests are in their privacy policies, and take into account individuals' enhanced right to object to the processing of their personal data. Where they are choosing to retain and process data for longer than they are required to do so, they should document the reasons.

Third party data sharing

The volume of data processed by financial institutions, combined with the increase in outsourcing back office functions, means that firms will have numerous flows of data to external vendors. This in turn may increase a firm's risk of a data breach. Firms must ensure that their vendors are complying with their GDPR obligations and that this is reflected in the contractual documentation. Indeed, under Article 28(3) of the GDPR the vendor contract must require the vendor to:

→ Only process personal data on documented instructions from the firm.

→ Protect the confidentiality of the personal data the vendor is processing.

→ Ensure the security of the data being processed (in accordance with Article 32 of the GDPR).

→ Ensure any further outsourcing contract the vendor enters into with another processor contains similar protections to those in its contract with the firm.

→ Assist the firm in responding to a data subject request.

→ Assist the firm with its obligations in the event of a personal data breach.

→ Delete or return all the personal data at the end of the contract if required by the firm.

→ Provide the firm all the information necessary to demonstrate compliance.

Firms should identify all vendors or third parties that are processing the personal data of the firm's customers and employees, use their best endeavours to verify that those vendors are complying with their obligations under the GDPR, and ensure that this is reflected in the contractual documentation. Firms could externally assess vendors' security and ensure that there is a common standard vendors are meeting. Firms should also require vendors to complete detailed questionnaires on their data infrastructure and storage. These assessments should not be one-off events either. Firms should periodically assess vendors to ensure they remain GDPR compliant and are maintaining market standards.

Firms will also likely want to seek indemnification from their vendors in respect of their data protection obligations. One should note, however, that there is currently no clear authority as to whether an indemnity which extended to a firm's own liability under data protection laws would fall foul of public policy grounds.

The right to be forgotten

The "right to be forgotten", as it has become known, can be found in Article 17 of the GDPR, which allows individuals "to obtain from the controller the erasure of personal data concerning him or her without undue delay" if there are specified grounds to do so. The first (and most widely known) of these grounds is that "the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed". Another relevant ground is where the individual "withdraws consent on which the processing is based…and there is no other legal ground for the processing".

However, the right to be forgotten is not absolute and Article 17(3) of the GDPR disapplies the right in a number of scenarios, including where the processing is necessary for:

→ Exercising the right of freedom of expression and information.

→ Compliance with a legal obligation.

→ The establishment, exercise or defence of legal claims.

Again, therefore, the existence of a regulatory obligation to retain data would trump the data subject's right of erasure, but again the difficulty arises where firms are going beyond what they are required to retain. A firm may also seek to justify refusing a request for erasure where a regulatory enforcement action has been commenced or is reasonably in contemplation.

Where firms receive a request by a customer to erase personal data, they should have in place processes by which they can identify what data they hold on that individual, where it is stored, and what it is used for. Firms should also be aware on which base they are processing

the data. A request for data erasure essentially means that the individual no longer consents to the processing of that data. Firms still relying on consent should erase the data if no other legal base for processing the data exists.

Firms should also be aware that the GDPR makes it easier for individuals to make a subject access request (SAR) and be informed of whether a firm is processing their personal data and be given a copy of that data, perhaps as a precursor to exercising the right to be forgotten. Firms may no longer charge a £10 administration fee (unless the request is "manifestly unfounded or excessive") and must now respond within a month rather than the current 40 days. As with the right to be forgotten, firms must ensure they are aware of what data they hold, know where it is held, and understand how to obtain a copy to provide to the individual. It may be helpful to prepare template letters to ensure all the requirements of responding to a SAR are met.

Privacy by design and privacy by default

One of the main aims at the heart of the GDPR is to put data privacy and firms' use of individuals' data at the heart of all the business. In this regard, the GDPR requires firms to take an approach known as "privacy by design".

Under the privacy by design approach, data controllers must consider the privacy risks and data protection compliance from the start of a project involving personal data. Such projects might include the building of new IT systems, developing new financial products, drafting new policies, and sharing data with third parties.

Article 25 of the GDPR implements "privacy by design" and requires data controllers to "implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of [the GDPR] and protect the rights of data subjects".

"Psudonymisation", one of the measures suggested by the GDPR, is defined as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person". One example of pseudonymisation would be replacing someone's name with a random ID number.

The ICO suggests using privacy impact assessments (PIAs) to implement privacy by design. A PIA is a process that assists organisations in identifying and minimising the privacy risks of new projects or policies. The ICO has also produced a code of practice and template document to assist firms conducting PIAs The code of practice describes the PIA process as follows:

- → Identifying the need for a PIA.
- → Describing the information flows.
- → Identifying the privacy and related risks.
- → Identifying and evaluating privacy solutions.
- → Signing off and recording the PIA outcomes.
- → Integrating the PIA outcomes back into the project plan.

The PIA should become part of a firm's procedures when starting a new matter. This will reduce the risk that firms breach the GDPR once the initial rush of GDPR awareness has faded.

Size of penalties and consequences of a breach

The headline-grabbing change is the increased level of fines that can now be levelled for breach of the requirements of the GDPR. Previously, the ICO could levy fines of up to £500,000 for data protection breaches; under the GDPR, the ICO will be able to levy fines of up to 4% of a firm's annual worldwide turnover or EUR 20,000,000, whichever is highest. The ICO has said that fines will be a last resort and that the penalties will not simply scale up once the GDPR comes into force. Nevertheless, the risk of a substantial financial penalty exists, particularly for egregious breaches and/or where there is detriment to data subjects on a large scale.

In order to mitigate this risk, firms' policies and procedures must focus not just on the day to day treatment of personal data, but also a firm's approach to dealing with a personal data breach. The GDPR requires that a firm classified as a data controller notifies the ICO "without undue delay and, where feasible, not later than 72 hours after having become aware of it…" and notifies the individuals affected "without undue delay". Firms should ensure that they have a clear protocol in place to identify individuals affected and implement protocols to notify the ICO.

This positive reporting obligation to the ICO is entirely new. Firms in the financial sector will of course continue to have their existing regulatory reporting obligations, and any disclosure to the ICO does not negate the need to inform the FCA and PRA of a data breach under Principle 11 of the FCA's Principles for Businesses or Fundamental Rule 7 of the PRA's Fundamental Rules. Firms should also be aware of the adverse publicity that will follow any data breach and should have a communications strategy in place to deal with this too.

Concluding thoughts

Following the implementation of the GDPR, there will necessarily be a degree of uncertainty in the market and a harmonisation of market practices and procedures. However, firms should be aware of the main areas of concern and ensure that they understand:

- What data is being held by a firm.
- What access third parties have to such data.
- The basis on which data is processed.

Financial institutions need to ensure that data protection is a high priority across a firm and is incorporated into all new ventures.